

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
10 May 2001 (10.05.2001)

PCT

(10) International Publication Number
WO 01/33851 A1

(51) International Patent Classification⁷: H04N 7/16, 7/167, 7/24

(21) International Application Number: PCT/US00/30215

(22) International Filing Date:
2 November 2000 (02.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/163,024 2 November 1999 (02.11.1999) US

(71) Applicant (for all designated States except US): THOMSON LICENSING S.A. [FR/FR]; 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): DUFFIELD, David, Jay [US/US]; 5459 Fall Creek Road, Indianapolis, IN 46220 (US). DIASCORN, Jean-Louis, Yves [FR/US]; 496 Arbor Drive, Carmel, IN 46032 (US). ESKICIOGLU, Ahmet, Mursit [TR/US]; 8235 Lakeshore Trail, Apt. # 125, Indianapolis, IN 46250 (US).

(74) Agents: TRIPOLI, Joseph, S. et al.; Thomson Multimedia Licensing Inc., P.O. Box 5312, Princeton, NJ 08540 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR ADDING A CONDITIONAL ACCESS SYSTEM

400

PID	DESCRIPTION	PACKETS PER 1000 INCOMING		PACKETS PER 1000 OUTGOING
000	PAT 230	5	NOT A PMT ENTRY. POINTS TO THE PMT FOR THIS SERVICE AT PID # 100. (ALSO POINTS TO ANY OTHER SERVICES ON THIS PHYSICAL CHANNEL.)	5
100	PMT 207	5	NOT A PMT ENTRY. THIS PID CONTAINS THE PMT PACKETS	5
101	VIDEO	850	NO CHANGES	850
102	AUDIO	110	NO CHANGES	110
110	NDS CA ECMS	10	NO CHANGES	10
111	IRDETO CA ECMS	10	PACKETS ARE REMOVED AND REPLACED WITH XCA LECMS ON PID 120	0
112	NAGRA CA ECMS	10	NO CHANGES	10
120	XCA CP ECMS	0	PACKETS ARE INSERTED WHERE CA PACKETS WERE REMOVED	10
121	CMPS CP ECMS	0	NO CHANGES	0

(57) Abstract: A method for adding a conditional access system to a digital audio/video transmission system that delivers content from a source to a security device associated with an audio/video processing device by providing at the broadcast source a datastream having system information data including an unused identifier reserved for security data associated with the additional conditional access system.

WO 01/33851 A1



(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

With international search report.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR ADDING A CONDITIONAL ACCESS SYSTEM**Field of the Invention**

The present invention relates generally to digital audio/video transmission systems,
5 and more particularly to a method which allows the addition of a conditional access system in
a digital audio/video transmission system without downstream modification of system
information tables in MPEG data.

Background of the Invention

10 ISO/IEC 13818-1 (Information Technology-Generic Coding of moving
pictures and associated audio information systems) is an international standard that specifies
the coding of one or more elementary streams of audio and video as well as other data into
single or multiple streams suitable for storage and transmission. A transport stream (TS)
combines one or more programs with one or more independent time bases into a single
15 stream. TS packets are 188 bytes in length. Each TS packet has a 4-byte header with a packet
ID (PID) that identifies the type of data contained in the packet. In addition to A/V packets, a
TS contains system information tables to demultiplex and present programs. A Program Map
Table (PMT) is a table that provides the mappings between the program numbers and the
elements that comprise them. It includes a list of PIDs associated with each program.

20 The Advanced Television Systems Committee (ATSC) has adopted the Simulcrypt
architecture for its Conditional Access (CA) system for terrestrial broadcast. In this
architecture, each service is transmitted with Entitlement Management Messages (EMMs) and
Entitlement Control Messages (ECMs) for a number of different proprietary systems. This
way, decoders using different CA systems can decode the service using a common framework
25 for signaling the different entitlement messages. EMMs carry private CA information

specifying authorization levels or services of specific decoders, whereas ECMs contain control words for descrambling authorized services. Each service is comprised of audio and video packets. Any one decoder picks out the packets it needs and ignores the others in the stream.

5 In a Simulcrypt based CA system, a digital audio/video processing system, such as a Digital Television (DTV), parses the PMT and extracts the service and ECM PIDs using a CA system identification (ID) obtained from the CA module. Normally, each CA module supports only one CA system, and therefore has only one CA system ID. The PIDs of the A/V packets and the PIDs of the ECMs carrying the Control Words (CWs) are sent to the CA
10 module, which descrambles programs having proper purchase entitlements.

Extended Conditional Access (XCA) is a copy protection system for providing local protection of audio and video content during transmission and storage in digital home networks. It specifies access and presentation devices to access, convert and display protected content. Removable security devices (converter and terminal cards) are recommended for
15 performing security related functions. In XCA, the descrambling keys are rebundled in an ECM which is protected by a unique local key. The decoder that receives content with local ECMs therefore may need to handle not only the content protected by its own particular CA system, but by XCA as well.

The National Renewable Security Standard (NRSS) provides a means for renewable
20 security to be employed with digital consumer electronics devices such as digital television receivers and digital VCRs. The security functionality is thus separated from navigational devices. When an NRSS security device receives protected content from its host device, it descrambles it, and sends it back to the host device. This link may also need to be protected.

In an ISO/IEC 13818-1 based system, a program may be scrambled in order to provide
25 a Pay TV service. The transport stream carries the programs, the ECMs and the PMTs. The

PMT has an entry for each CA system that protects the program. Each entry contains the CA_system_id, the PIDs of the scrambled streams and the PID of the ECMs that contain the keys to descramble the program.

If the receiving device is also a transformation device which can either add an extra CA system, or replace one (for copy protection, for example, like XCA does), then this device needs to output a transport stream where the PMT has an entry for that new CA system. The receiving device may acquire each and every PMT that is present in the original transport stream, process them, add the entry for the extra CA system and then insert the modified PMTs in the output transport bitstream.

The aforementioned process can be very burdensome due in part to the limited processing power of receiving devices. Furthermore, processing complexities increase due to the fact that PMTs may span more than one transport packet. Thus, adding an entry may mean adding a packet, which in turn poses a multiplexing problem, as the bitstream may already be full or the time stamps may need to be adjusted. A method which overcomes these problems is highly desired.

Summary of Invention

A method for adding a conditional access system comprises providing at the broadcast source a data stream having a portion thereof reserved for insertion of security data associated with the additional conditional access system. The additional CA system is declared during the original transport stream creation at the broadcast source by adding an entry in the PMT. This entry defines a unique PID for the ECMs. The PID reserved for the extra CA system ECMs is not used in any other way, and the transport stream arriving at the receiver device will not contain any packets having the reserved PID. The present invention implements at the broadcast source sending 'dummy' entries for data streams that are not present in the CA

protected broadcast, thereby minimizing the PMT processing required for each conversion of the service data. A correct PMT is thus output from the receiving device without the need to modify/update tables.

The present invention is embodied in a method of operating a security device in a conditional access system comprising receiving a datastream having system information data including an unused identifier reserved for security data associated with the additional conditional access system; and inserting into the data stream the security data associated with the additional conditional access system.

10 Brief Description of the Figures

Figure 1 illustrates an exemplary embodiment of a network adapted to receive content from a broadcasting source and provide copy protection using XCA and NRSS copy protection systems.

Figure 2 illustrates a block diagram of the functional elements and processing flow associated with adding a conditional access system according to an aspect of the present invention.

Figure 3 illustrates a block diagram of the processing associated with conversion of content by a security device for a conditional access system according to an aspect of the present invention.

Figure 4 illustrates an exemplary embodiment of a program map table useful in carrying out the present invention.

Detailed Description of the Invention

Figure 1 illustrates a network 10 that receives content via a transport stream from a broadcasting source, i.e. via content source 20, and provides protection with XCA (described

herein). The content source 20 can provide content 22 of economic value, whether from tape, DVD, cable, satellite or terrestrial broadcast, for example. The content 22 typically includes A/V content, which is protected and supplied to subscribers of a private CA network. The subscribers who purchase, or are otherwise entitled to receive the content 22, are supplied
5 with necessary keys for descrambling the content 22. According to the embodiment of Figure 1, the content source 20 can provide this CA content 22 to an access device 30, recording device 40 and/or presentation device 50, for example.

Access device 30 can take the form of a set-top box. The access device 30 operates in conjunction with a removable security device such as an XCA/NRSS converter card 35 to
10 create XCA protected content in CA/XCA content 33 from the CA content 22. Recording device 40 can take the form of a Digital VHS (DVHS) or DVD recorder. The recording device may or may not be provided with a removable security device such as converter card 45 analogous to the converter card 35. Presentation device 50 can take the form of a DTV, and operate in conjunction with removable security device XCA/NRSS terminal card 55 for
15 descrambling CA/XCA protected content.

Figures 2-4 provide schematic illustrations of the processing associated with forming the transport stream 22 for input into an audio/video processing device 30 and associated security device 35 and subsequent output of the transport stream 33. Note that the present invention applies to ISO/IEC 13818-1 compliant data systems, including conditionally
20 accessed digital TV systems like ATSC, DVB and ARIB (whether, Terrestrial, Satellite, Cable SMATV, or MMDS).

As shown in Figure 2, the broadcast source 20 includes a source of content which is encoded via encoder 201 (for example, a PES encoder) and conventional multiplexer/scrambler module 204. A radiating source such as antenna 208 communicates the
25 content to audio/video processing device (e.g. receiver) 30 and corresponding security device

35 (see Figs. 1, 3). Program Map Table (PMT) 207 illustrated therein is associated with transport stream 22. In PMT 207, there is shown an association 207A of CA_system_id 1 with corresponding ECM PID 1, and association 207B of CA_system_id 2 with corresponding ECM PID 2. In order to add a CA system, an additional CA_system_id is declared at the
5 broadcast site 20 via an additional table entry 207C into the PMT associating extra_CA_system_id with corresponding extra_ECM_PID. The additional PID is preferably a previously unused PID reserved for the ECM of the added or extra CA system. That is, the PID is not used for transport packets before the bitstream gets transformed at the receiver. Note that the transport stream 22 shown in Figure 2 (and Figure 3) does not contain the extra
10 ECMs. At the receiver 30, the PID for the ECM for the extra CA system is extracted from the PMT 207. The receiver then generates the ECMs with that PID and inserts them into the datastream to provide output datastream 33.

Referring more particularly to Figures 3 and 4, there is depicted an exemplary processing flow of the datastream or bitstream 22 as it would enter and exit a security device
15 35 such as an Irdeto/XCA CA module. The CA module converts the content to XCA using the entries provided in PMT 207.

As shown in Fig. 4, table of PID entries 400 includes an entry for the Program Association Table (PAT) 230. The PAT 230 is predefined in MPEG to be located on PID 000 (0x0000) and points to all the PMT PIDs. There is one PMT for each service. PMT 207
20 includes entries for all the PIDs that make up a given service (in this case video, audio, CA, and eventually, CP).

Two "dummy" entries 120, 121 exist in the PMT 207 as it is sent over the network to security device 35 (Fig. 3). The mapping determines how XCA and CMPS should provide copy protection. In the example depicted herein, it is understood that the service provider
25 authorizes XCA and CMPS as copy protection systems. This also provides a mechanism for

the interoperation of more than one cooperating CP system. The two CP system PIDs 120, 121 are not used in the network broadcast data stream shown in Fig. 3 (i.e., there are no packets sent on these PIDs). When the CA module descrambles the content and converts it to a CP system, the CA ECM packets (PID 111 in Fig. 4) are removed and replaced with the CP system packets (PID 120) at the same locations in the bitstream, as illustrated in Fig. 3.

Addition of the dummy entries to the PMT 207 has the following benefits: First, the provider can ensure that there are no collisions by abstaining from sending data on the PIDs specified for CP ECM data. This way, the CA module does not have to pick a PID and run the risk of 'colliding' with another PID that the broadcaster is using. Second, if the broadcaster does not want to be program copied, he does not put the CP entries into the PMT. If the pirate wants to tape this program, he will have to edit the PMT properly in addition to all other requirements for making a recording. Note that the PMT 207 is valid both before and after the CA/CP conversion.

Note also that a recording device such as that depicted in Figure 1 will also not have to modify any entries in the PMT. (Even in the systems where recording devices need to change CP system data flags.) The CP system control flags will be located in the CP ECM PID packets and can be modified there.

The present invention also contemplates the possibility of 'reuse' of the CA system PID for the CP system data. However, in a simulcrypt system, this makes it difficult to find the CP system ECMs. Either the PMT must be changed so that it points to the XCA ECMs properly, or a device trying to find the XCA ECMs must know which CA system initially descrambled the content. In addition, if the stream is to be ISO/IEC 13818-1 compliant, modification of the PMT may also be required.

8
CLAIMS

1. A method for adding a conditional access system to a digital audio/video transmission system that delivers content from a source to a security device associated with an audio/video processing device, said method comprising:

5 providing at said broadcast source a datastream having system information data including an unused identifier reserved for security data associated with said additional conditional access system.

2. The method according to claim 1, further comprising said security device providing
10 said security data using said unused identifier in said data stream.

3. The method according to claim 1, wherein said security data includes entitlement control messages.

15 4. The method according to claim 1, wherein said providing step further comprises inserting at said broadcast source at least one entry into a program map table associating said additional conditional access system with a packet identifier, said packet identifier being associated with entitlement control messages.

20 5. A method of operating a security device in a conditional access system comprising:
receiving a datastream having system information data including an unused identifier reserved for security data associated with said additional conditional access system; and
inserting into said data stream said security data associated with said additional conditional access system.

6. The method according to claim 5, wherein said additional conditional access system comprises a copy protection system.

7. The method according to claim 5, further comprises parsing a map table associating
5 said unused identifier with said additional conditional access system to obtain said security data for insertion into said data stream.

8. The method according to claim 5, wherein said security device does not update said program map table for said additional conditional access system.

10

9. A method for creating system information tables for an additional conditional access system sent in a datastream from a content source to a security device, said method comprising

providing table entries having an unused identifier reserved for security data
15 associated with said additional conditional access system.

10. The method according to claim 9, further comprising inserting at said security device security data associated with said identifier.

20 11. A method for adding a conditional access system to a digital audio/video transmission system that delivers content from a source to a security device associated with an audio/video processing device, said method comprising:

providing at said broadcast source a datastream having a portion reserved for downstream insertion of security data.

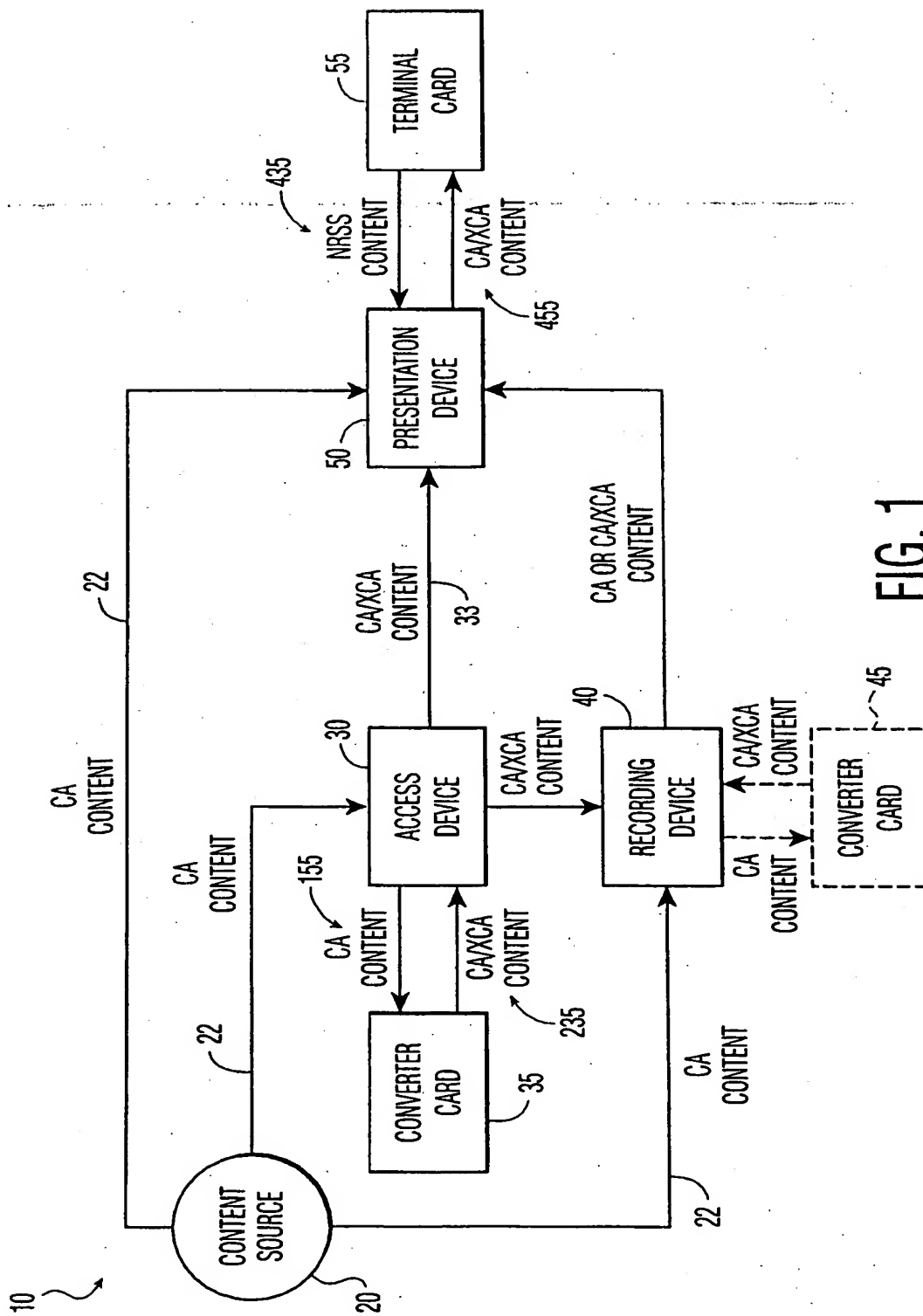


FIG. 1

2/4

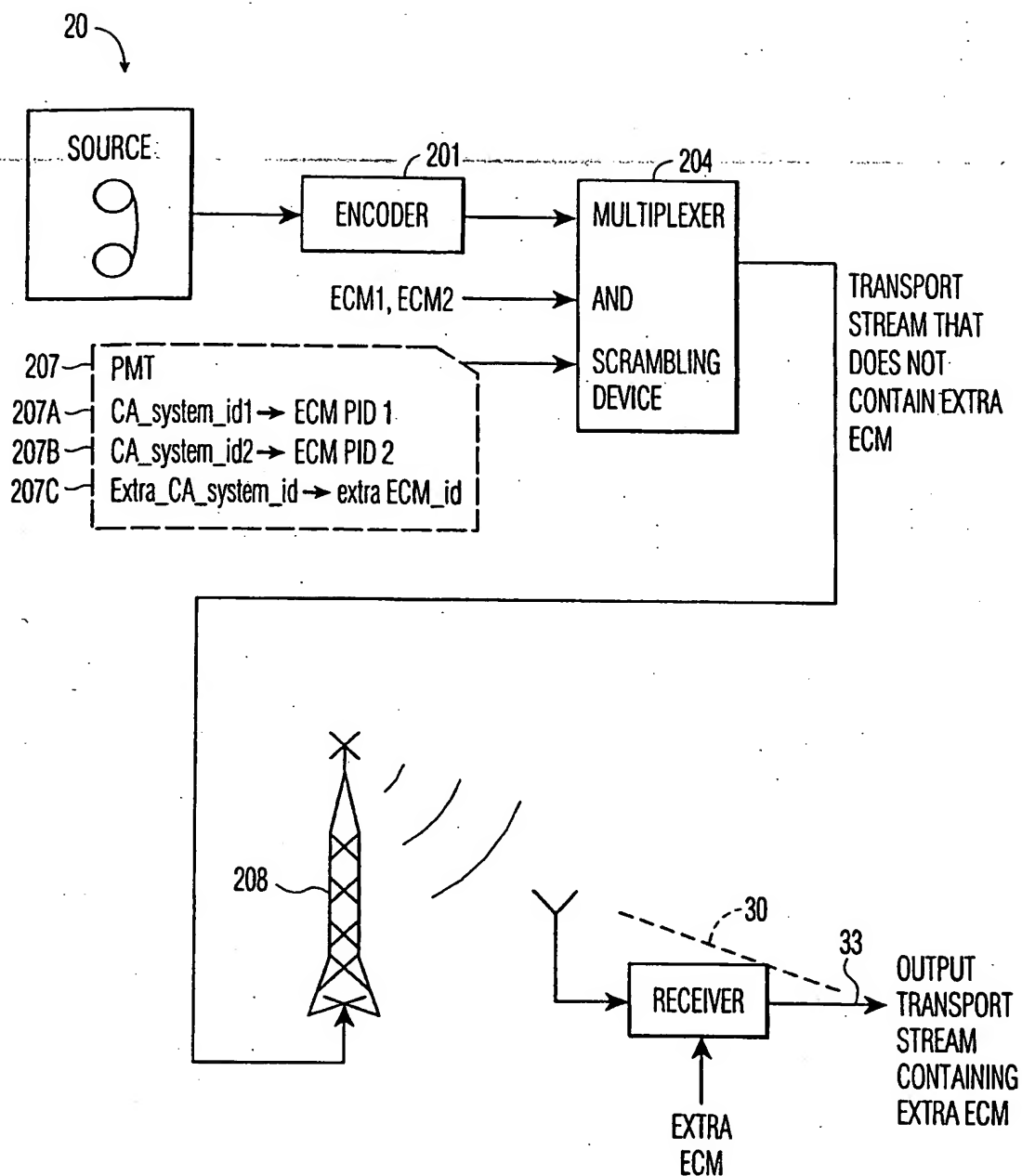


FIG. 2

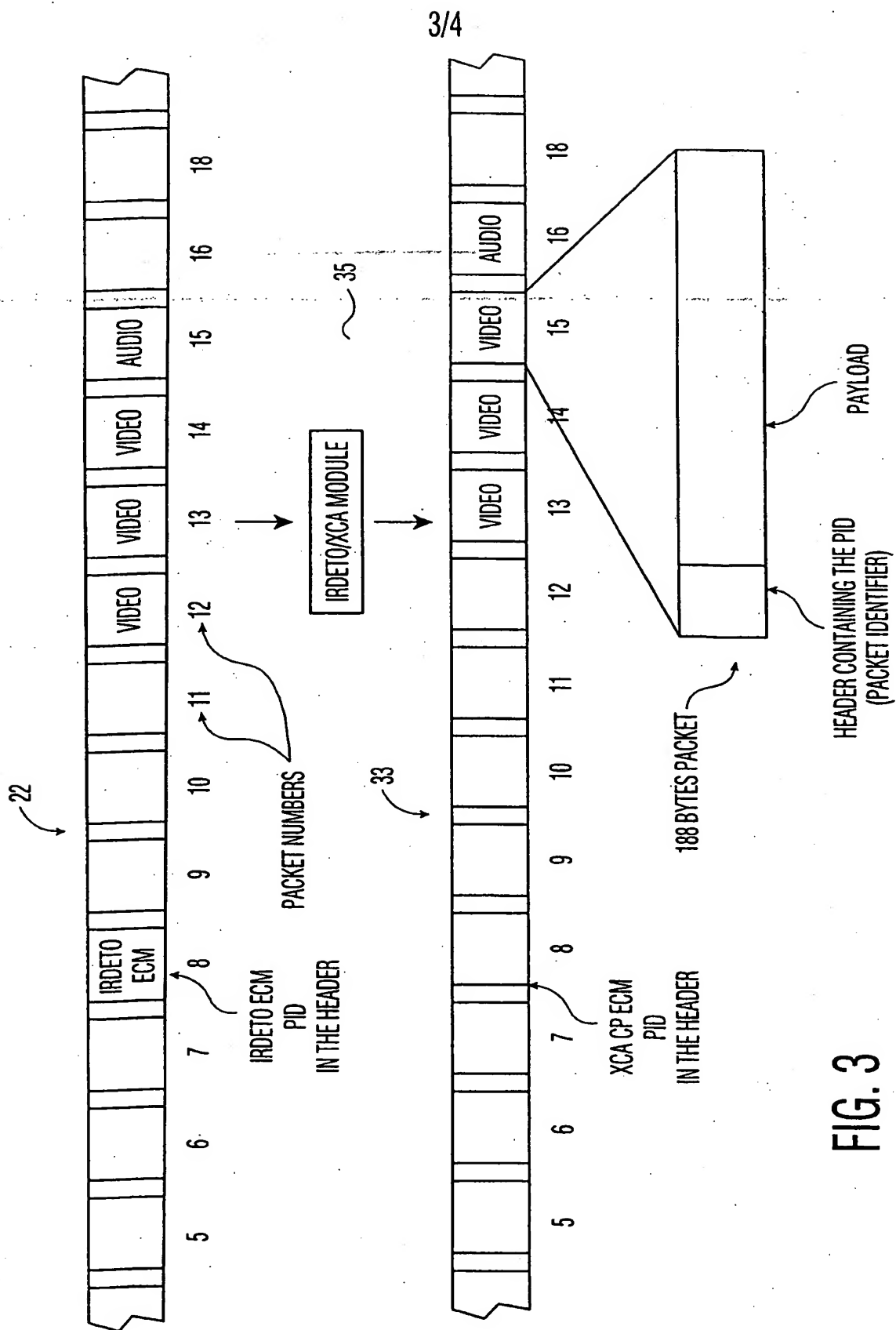


FIG. 3

4/4

400
↘

PID	DESCRIPTION	PACKETS PER 1000 INCOMING		PACKETS PER 1000 OUTGOING
000	PAT <u>230</u>	5	NOT A PMT ENTRY. POINTS TO THE PMT FOR THIS SERVICE AT PID # 100. (ALSO POINTS TO ANY OTHER SERVICES ON THIS PHYSICAL CHANNEL.)	5
100	PMT <u>207</u>	5	NOT A PMT ENTRY. THIS PID CONTAINS THE PMT PACKETS	5
101	VIDEO	850	NO CHANGES	850
102	AUDIO	110	NO CHANGES	110
110	NDS CA ECMs	10	NO CHANGES	10
111	IRDETO CA ECMs	10	PACKETS ARE REMOVED AND REPLACED WITH XCA LECMs ON PID 120	0
112	NAGRA CA ECMs	10	NO CHANGES	10
120	XCA CP ECMs	0	PACKETS ARE INSERTED WHERE CA PACKETS WERE REMOVED	10
121	CMPS CP ECMs	0	NO CHANGES	0

FIG. 4

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 00/30215

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04N7/16 H04N7/167 H04N7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 420 866 A (WASILEWSKI ANTHONY J) 30 May 1995 (1995-05-30) abstract column 10, line 8 - line 33; figures 3-5 column 12, line 59 - line 66	1,5,9,11
A	WO 99 22372 A (SONY ELECTRONICS INC) 6 May 1999 (1999-05-06) abstract	1,5,9,11



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *Δ* document member of the same patent family

Date of the actual completion of the international search

14 February 2001

Date of mailing of the international search report

20/02/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Dockhorn, H

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 00/30215

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5420866 A	30-05-1995	AU 687844 B	05-03-1998
		AU 7220994 A	17-10-1995
		CA 2186368 A,C	05-10-1995
		JP 2940639 B	25-08-1999
		JP 9511369 T	11-11-1997
		WO 9526597 A	05-10-1995
WO 9922372 A	06-05-1999	AU 1103599 A	17-05-1999
		EP 1012840 A	28-06-2000